NEWSLETTER

I.T.INSIGHTS NEWSLETTER - ISSUE #05 - FEBRUARY 2025

Cyber Threats Escalate

i.t. 30 now

We Make It Look Easy

RANSOMWARE ATTACKS ON CRITICAL INFRASTRUCTURE SURGE, DEMANDING VIGILANCE

Ransomware attacks targeting critical infrastructure are escalating, posing an unprecedented threat to essential services like energy, water, and healthcare. A successful attack can cripple operations, endanger lives, and inflict massive financial damage. The interconnected nature of modern infrastructure makes it vulnerable, and recent incidents highlight the urgent need for robust cybersecurity measures to protect these vital systems.

Critical infrastructure has become a prime target for ransomware gangs due to its essential nature and often outdated security systems. These organizations are willing to pay hefty ransoms to restore services quickly, making them lucrative targets. The rise of ***ransomware-as-a-service (RaaS)*** has further lowered the barrier to entry, enabling less sophisticated actors to launch devastating attacks. A recent report indicates a 40% increase in ransomware attacks on critical infrastructure in the past year.

However, the impact of ransomware attacks on critical infrastructure extends far beyond the targeted organizations.

Disruptions to energy or water services can affect entire communities, causing widespread economic losses and social unrest. Hospitals and healthcare providers are particularly vulnerable, as attacks can compromise patient data and disrupt critical medical services.

The cost of recovery from these attacks can be staggering, often involving millions of dollars in ransom payments, system upgrades, and legal fees. SMBs who support critical infrastructure are also targets and must ensure they are up to the task.

In February 2025, CISA released an alert detailing a new ransomware variant targeting industrial control systems (ICS) used in water treatment

facilities. According to the alert, the ransomware exploits known vulnerabilities in outdated software and emphasizes the urgent need for patching and security updates. The Cybersecurity and Infrastructure Security Agency (CISA) added several vulnerabilities to its Known Exploited Vulnerabilities Catalog. Read More

To mitigate the risk of ransomware attacks on critical infrastructure, businesses should implement a multi-layered security approach that includes:

- ***Regular security audits:*** Identify vulnerabilities and weaknesses in your systems and networks.
- ***Employee training:*** Educate employees about phishing scams and other social engineering tactics used by attackers.
- ***Strong passwords and MFA:*** Prevent unauthorized access to sensitive systems and data.
- ***Patch management:*** Keep software and firmware up to date to address known vulnerabilities.
- ***Network segmentation:*** Isolate critical systems from the rest of the network to limit the impact of a successful attack.
- ***Incident response plan:*** Develop a detailed plan for responding to a ransomware attack, including procedures for containment, eradication, and recovery.
- ***Backups:*** Regularly back up critical data and store it offsite to ensure that you can restore your systems in the event of an attack.

Protecting critical infrastructure from ransomware attacks requires a collaborative effort between government agencies, private sector organizations, and individual citizens. By implementing robust cybersecurity measures and sharing threat intelligence, we can collectively strengthen our defenses against these evolving threats.

Is your business at risk? Contact us for expert IT solutions and cybersecurity support.

Schedule a Consultation

CLIENT SUCCESS STORY

EMPLOYER ADVOCATES BOOSTS SECURITY & EFFICIENCY WITH I.T.NOW

Employer Advocates is a third-party administrator specializing in assisting companies in the unemployment process. This leading HR solutions provider, faced growing IT challenges as they scaled their business. Protecting sensitive client data and maintaining operational efficiency were paramount to their success in the competitive HR landscape. Before partnering with i.t.NOW, Employer Advocates struggled with outdated systems that lacked comprehensive cybersecurity measures. This exposed them to potential data breaches and compliance risks, hindering their ability to provide secure and reliable services to their clients.

How i.t.NOW Helped:

i.t.NOW implemented a robust suite of solutions, including advanced threat protection, 24/7 monitoring, and regular security assessments.

By transitioning Employer Advocates to a secure cloud environment, i.t.NOW enhanced data accessibility and collaboration while fortifying their overall security posture.

Helpdesk support ensures minimal disruptions for their employees.

Key Results:

Since partnering with i.t.NOW, Employer Advocates has experienced:

- Enhanced cybersecurity posture with proactive threat detection
- Improved operational efficiency through streamlined IT management
- Reduced risk of data breaches and compliance violations
- Allowed Employer Advocates to focus on growing the business

EMPLOYER ADVOCATES | CPA

"i.t.NOW has been instrumental in enhancing our IT security and operational efficiency. Their proactive approach and expertise have given us peace of mind, knowing our systems are protected and running smoothly. The level of service and commitment from i.t.NOW has allowed our team to focus on strategic initiatives."

— Steve Van Valkenburgh, COO Employer Advocates

UTAH'S SENATE BILLS FOR DATA CENTERS

As cloud computing continues to thrive, Utah's Senate is addressing the energy demands of new data centers through proposed legislation. This development is crucial for any company looking to capitalize on cloud technologies while ensuring sustainable energy practices.

Two competing Senate bills aim to set procedures for servicing high-energy data centers without straining resources for existing customers. SB132 focuses on allowing direct contracts with large users, while SB227 promotes renewable resource usage without specifying requirements. The challenge is to ensure that energy costs for data centers do not affect local consumers' utility rates.

Why it Matters: Companies considering cloud solutions must pay attention to these developments, as energy regulations may impact service availability and costs. Engaging with local policymakers can help ensure their needs are represented as these regulations evolve.

Read more
Published on February 14, 2025

NEW RISKS FOR BUSINESSES -AI THREATS

As we progress deeper into 2025, concerns are growing around the use of AI in cyber threats. Emerging AI technologies present both opportunities and significant risks.

The emergence of agentic AI, capable of independent decision-making, is raising alarms due to its potential use in sophisticated cyberattacks. Malicious actors may leverage agentic AI to execute elaborate phishing campaigns and exploit vulnerabilities in small business networks. Additionally, over 57 nation-state actors are now using AI to augment their cyber operations, increasing risks related to espionage and data breaches.

Why it Matters: It's critical for companies to enhance their cybersecurity frameworks to counteract these intelligent threats. Investing in AI security tools and increasing awareness of AI-driven risks will help protect sensitive business data from potential exploitation.

Read more
Published on February 4, 2025

EXCITING INNOVATIONS IN CLOUD COMPUTING

Cloud computing continues to evolve rapidly, with significant enhancements and investments this February. These developments are particularly relevant for SMBs looking to optimize operations and enhance security.

Highlights include AWS's announcement of new security features for their services, such as enhanced protection capabilities in AWS WAF and improved IAM for server-side rendered applications. Additionally, Alibaba plans to invest $52 billion in AI and cloud technology over the next three years, aiming to strengthen its position against major players like AWS. These advancements facilitate improved resource management and security, vital for businesses migrating to the cloud.

Why it Matters: It's critical for companies to enhance their cybersecurity frameworks to counteract these intelligent threats. Investing in AI security tools and increasing awareness of AI-driven risks will help protect sensitive business data from potential exploitation.

Read more
Published on February 24, 2025

MANAGED IT SERVICES PRICING CALCULATOR & CHECKLIST

Navigating the complexities of IT service pricing can be daunting for small and medium businesses. With varying quotes and service models, it's essential to have a clear understanding of what you truly need. The Managed IT Services Pricing Calculator & Checklist is here to simplify the decision-making process for your organization.

- Gain insights into the various components of managed IT services and tailored cost estimates.
- Use the comprehensive checklist to evaluate your specific IT needs against provider capabilities.
- Compare different service models and pricing structures to find the best fit for your business.
- Understand the critical importance of security, compliance, and proactive IT support in service selection.

This resource provides the essential framework to ensure you don't overlook critical IT service elements, potentially saving you time, money, and reducing risk.

Download the Guide Here!

MALWARE & BRUTE FORCE ATTACKS

In February 2025, the notorious North Korean hacking group, Lazarus, launched a series of malware campaigns targeting software developers and cryptocurrency users. As cybercriminals increasingly adapt their strategies, these recent attacks can have disastrous implications for vulnerabilities within the software supply chain and small to medium-sized businesses (SMBs) engaging in technology-related work. Safeguarding digital assets is paramount as these threats evolve.

The Lazarus Group's attacks are multifaceted. Their recent **Operation Marstech Mayhem** deploys malware called Marstech1 through compromised open-source repositories, primarily on GitHub. Victims encounter malicious JavaScript embedded in legitimate-looking packages, leading to system infection and cryptocurrency wallet data theft.

Additionally, in the **Deceptive Development Campaign**, fake job offers on platforms like Upwork lure developers to click on trojanized repositories. Once executed, these malicious scripts harvest sensitive information, compromising users globally. So far, 233 confirmed cases have emerged across multiple regions, underscoring the wide-reaching effects of this threat.

With these advanced tactics, SMBs reliant on software development and cryptocurrency transactions must brace for more frequent and sophisticated attacks. Experts warn this trend may proliferate, with many unsuspecting developers falling prey to such social engineering schemes, especially as organizations adapt to remote and hybrid work models.

Read More

February 2025 also saw the emergence of the **SparkCat malware campaign**, a new threat designed to infiltrate both Android and iOS devices. This sophisticated Trojan uses advanced optical character recognition (OCR) technology to steal sensitive cryptocurrency wallet recovery phrases. As malware increasingly blends into mobile apps,

companiess and their employees need to be vigilant against this evolving threat.

SparkCat is cleverly disguised, appearing in seemingly legitimate applications on both major app stores. Once installed, the malware requests access to the user's photo library and employs OCR to scan for cryptocurrency recovery phrases stored in images. It utilizes the Google ML Kit library, a legitimate tool for text recognition, to identify information crucial for accessing digital wallets. Affected applications have reportedly been downloaded over 242,000 times from Google Play, raising concerns about the extent of this threat.

With the rapid proliferation of cryptocurrency, anticipated attack levels will likely increase. Researchers predict mobile users, particularly those involved with cryptocurrency trading, will be prime targets, underscoring the need for heightened awareness and protective measures.

Read More

A massive brute-force attack campaign has emerged in February 2025, involving a staggering 2.8 million IP addresses targeting various networking devices, including VPNs and firewalls. This large-scale attack poses a significant risk to organizations that utilize vulnerable internet of things (IoT) devices, emphasizing an urgent need for enhanced cybersecurity protocols.

This campaign uses compromised devices to form extensive botnets, executing systematic login attempts against network security devices. By employing residential IP addresses, attackers disguise malicious traffic as legitimate, complicating detection efforts for cybersecurity teams. The high volume of login attempts can lead to service disruptions, data breaches, and potential ransomware deployment if successful.

As this campaign demonstrates, brute-force tactics are becoming increasingly prevalent in the cybersecurity landscape. The growing interconnectivity of IoT devices means that successful breaches could compromise entire networks. SMBs must prepare for a future where these types of attacks are routine, requiring constant vigilance and advanced security measures.

Read More

An Introduction to Microsoft 365 Copilot

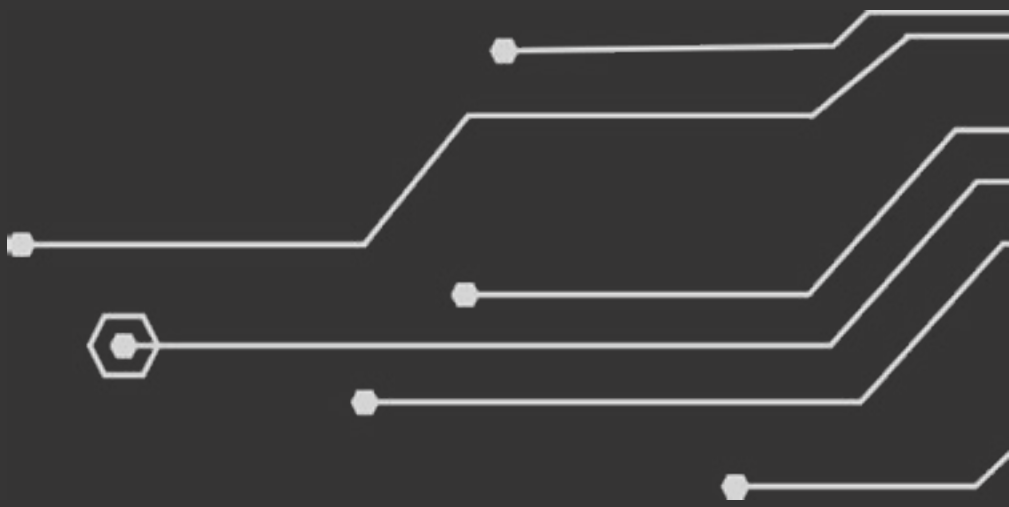
Microsoft 365 Copilot is transforming how businesses leverage AI to streamline operations, boost efficiency, and enhance productivity. This webinar, featuring expert Austin Hampton, provides a deep dive into Copilot's capabilities and practical applications. Learn how to optimize your workflow, maximize your investment in Microsoft 365, and integrate AI seamlessly into your business processes. **Watch The Replay!**

Key takeaways included:

- **The Value of Generative AI** – Understand how AI, particularly Copilot, enhances productivity by overcoming skill gaps and enabling faster, higher-quality work.
- **How AI Works** – Learn the basics of large language models, how Copilot generates responses, and why structured prompting is key to getting the best results.
- **Real-World Use Cases** – See how businesses are leveraging Copilot across departments like marketing, operations, and customer service to save time and improve decision-making.
- **Security & Compliance** – Discover why Microsoft Copilot is the best AI tool for businesses concerned about data privacy, security, and regulatory compliance.
- **Practical Implementation** – Get actionable insights on how to integrate Copilot into your daily workflows and maximize its ROI. **Make sure to join the Copilot workshop on March 20th!**

Generative AI is revolutionizing business operations, but many companies struggle to effectively implement and utilize these tools. This session equips business leaders with the knowledge and strategies needed to turn Copilot into a powerful asset. With real-world examples, structured guidance, and a focus on secure AI usage, this webinar ensures you walk away with foundational knowledge to start leveraging Copilot today.

Book an Appointment with Mike Herrington, VP of Sales & Marketing
If you have questions or would like personalized advice on strengthening your IT infrastructure, our team is here to help. Schedule a call back with Mike Herrington, VP of Sales & Marketing, to explore how we can protect your business. **Schedule an appointment here**



(801) 562-8778
Sales: (801) 859-2171

help@itnow.net

2436 W 700 S
Pleasant Grove, UT 8406